RFC-0010 FedRAMP Scope Interpretation Technical Assistance

Thursday, May 15th, 2025

Background

OMB Memorandum M-24-15 "Modernizing the Federal Risk and Authorization Management Program (FedRAMP) updated FedRAMP's scope, defining categories of services excluded from its requirements. To ensure consistent application of these exclusions across agencies, the memorandum requires the publication of clarifying guidance, stating in section 3 "*FedRAMP, in consultation with OMB, will publish guidelines for interpreting the categories above, with supporting examples that clearly illustrate what types of services are in and out of scope.*"

The information is provided for public awareness. Reference to any commercial product does not constitute endorsement by GSA. For more information, please see FedRAMP Disclaimers.

Introduction

M-24-15 "Modernizing the Federal Risk and Authorization Management Program (FedRAMP) establishes that agencies must apply FedRAMP when acquiring cloud services to create, collect, process, store, or maintain Federal information on behalf of a Federal agency, unless the service meets specific exclusion criteria outlined in the policy. This requirement enables standardized security assessment reuse and consistent monitoring across the federal government, promoting efficiency and enhancing security posture.

FedRAMP does not apply to all internet-based services used by agencies. M-24-15 Section 3 clearly defines specific categories of cloud services that are out of scope. Furthermore, agencies may use the same service offering differently based on mission needs, and each agency must determine FedRAMP applicability based on their specific implementation, use case, and risk profile.

This technical assistance clarifies the initial step of determining if FedRAMP requirements apply to a cloud service, based on the agency's specific use and the out-of-scope categories defined in M-24-15. While M-24-15 includes various processes and flexibilities for services requiring authorization, this guidance focuses solely on interpreting the scope exclusions.

Best practices and technical assistance MUST NOT be used as a checklist. All examples are for discussion purposes ONLY. This technical assistance is designed for reasonable people to have reasonable discussions about FedRAMP applicability based on their specific use of a cloud service.

This Technical Assistance document will be continuously updated to reflect evolving interpretive needs based on M-24-15's scope requirements. This includes updates to reflect any additional excluded categories identified by the FedRAMP Board with Federal CIO concurrence, or exceptions made by the FedRAMP Director with OMB approval.

Determining FedRAMP Scope

This guidance provides practical examples to help agencies navigate FedRAMP applicability decisions to ensure consistent implementation of M-24-15 across the federal government. The examples below illustrate how to interpret each of the out-of-scope categories defined in Section 3 of the OMB Memorandum. This guidance is not intended to be a complete listing of all possible examples or exclusions. Agencies must perform their own analysis and may find that some use cases may fall into multiple exemption categories outlined below

Information systems that are only used for a single agency's operations, hosted on cloud infrastructure or platform, and are not offered as a shared service or do not operate with a shared responsibility model;

When FedRAMP Doesn't Apply: The service is exclusively for a single agency's operations and not intended for reuse or reconfiguration by other agencies.

Key Tests:

- Single agency operational and configuration responsibility
- No assessment to reuse

Examples:

- Agency custom applications deployed to FedRAMP authorized IaaS
- Agency deployed instances of an app from a FedRAMP authorized PaaS vendors App Storefront
- Agency mission systems operated by a single agency with no shared operation or configuration responsibility

Out of Scope Detailed Example - Data.gov: GSA operates data.gov, a cloud hosted platform which allows agencies to share open datasets. While multiple agencies can contribute datasets, GSA maintains full responsibility for the systems configuration, operations, and authority to operate.

Analysis: Single operator; no shared platform responsibility.

In Scope Detailed Example - USDA AgCloud Managed Platform Services (AMPS): AMPS is a fully-managed DISC platform designed to give customers a supported and secure way to cloud computing. AMPS includes security services, patching services, administration services, and inheritable Authority to Operate (ATO) security controls for these managed services. Simply stated, AMPS provides the infrastructure on which customers may deploy their applications.AMPS provides a standardized, secure cloud platform that allows agencies to quickly deploy applications without managing the underlying IT infrastructure. By offering a shared, pre-configured environment with consistent security standards, AMPS assumes responsibility for the underlying platform, while customer agencies manage their applications.

Analysis: Reusable platform; shared responsibility model.

Social media and communications platforms used in accordance with agency social media policies

When FedRAMP Doesn't Apply: The service is not an authoritative repository for federal information, and its unavailability would not result in the loss of federal information.

Key Tests:

- Used in accordance with agency social media policies including compliance with Federal Records Act
- Primary purpose is external communication
- Not used as an authoritative source for federal information
- All federal information in the communication platform is intended for public use

Examples:

- Agency social media accounts (e.g., X, Facebook/Meta) including platform AI features (like content suggestions, public analytics, and sentiment analysis) that do not respond on behalf of the agency
- Scientific collaboration platforms (protocols.io)

Out of Scope Detailed Example - Scientific Collaboration: Agency researchers use protocols.io to communicate with the scientific community and share information. If protocols.io went away, the agency wouldn't lose any federal information so the platform isn't within the scope of FedRAMP.

Analysis: External communication using public information; not an authoritative source.

In Scope Detailed Example - Government Collaboration: Agency teams use collaboration platforms (e.g., Slack, Teams) for internal and cross-agency work, processing and storing sensitive, non-public federal information . Handling this information on behalf of agencies necessitates FedRAMP authorization.

Analysis: Handles internal, non-public federal information.

Search Engines

When FedRAMP Doesn't Apply: The search engine is used primarily for public information discovery and does not store, index, or maintain internal federal information on behalf of the government.

Key Tests:

- Primary function is public information discovery
- Does not collect or maintain federal information for agencies
- Users instructed not to input sensitive federal information

Examples:

- Public web search engines (e.g., Google, Bing, Lycos) using only public or non-sensitive federal information
- Public AI Chatbots (e.g., ChatGPT, Claude, Grok) using only public or non-sensitive federal information

Out of Scope Detailed Example - AI search chatbot: An agency uses a public AI Chatbot search to troubleshoot technical issues with a video conferencing system. Search queries of public or non-sensitive federal information may be logged by the vendor, but not FOR the agency. Because no internal data is accessed or trained on, FedRAMP doesn't apply.

> **Analysis:** Searches public information; does not collect or maintain internal federal information for the agency.

In Scope Detailed Example - Internal Data Search: An agency uses a shared cloud service to index and search internal repositories containing non-public federal information (e.g., documents, emails, databases). Because the service collects, processes, and maintains internal federal information on behalf of the agency, FedRAMP authorization is required.

> **Analysis:** Collects, processes, and maintains internal agency data for the agency.

Widely available services that provide commercially available information to agencies, but do not collect Federal information

When FedRAMP Doesn't Apply: The commercial information service does not collect or maintain federal information on behalf of the government.

Key Tests:

- Provides commercial services to agencies and the general public
- May temporarily process federal information (such as an address) to provide a response, and may maintain records of past requests, but does not collect or maintain federal information for the government
    - The agency does not require the service to retain or provide access to this information after the transaction or service delivery is complete
- Risk of unexpected exposure of federal information is accepted because the positive impact on the agency's mission is greater than the impact of the government's use of the system being exposed

Examples:

- Map services
- Public Certificate Authorities (e.g., Let's Encrypt, DigiCert) and DNS Resolvers
- Document and Address verification services
- Non-IT service providers such as airline ticketing or ride sharing systems

Out of Scope Detailed Example - Janitorial Services Scheduling: An agency sends building information and access information to a cloud scheduling portal used by their janitorial service company. The company uses the information to ensure that buildings are serviced and that janitors can access the building.

Analysis: Acquired non-IT service; cloud tool use is incidental; does not maintain federal information for the agency.

Out of Scope Detailed Example - Verification Services: An agency uses an address-validation service API which returns a true/false "match" and then discards the data. The service doesn't retain the federal information and there is little risk as the service is authoritative for the information provided (addresses), making it a service that falls outside the FedRAMP scope.

Analysis: Provides commercial data; temporarily processes federal information; does not maintain federal information for the agency.

In Scope Detailed Example - Verification Services (Identity): An agency uses a cloud Identity Verification service requiring users to submit PII. The service collects, processes, and stores this sensitive federal information (PII) on behalf of the agency to perform identity proofing and for later review. Maintaining federal PII for an agency function necessitates FedRAMP authorization.

Analysis: Collects and stores sensitive federal PII on behalf of the agency.

Ancillary services whose compromise would pose a negligible risk to Federal information or information systems, such as systems that make external measurements or only ingest information from other publicly available services

When FedRAMP Doesn't Apply: The agency determines, through a specific risk analysis, that the compromise or failure of the ancillary service would pose a negligible risk to federal information or information systems based on the agency's specific use. This determination may vary by agency and use case.

Key Tests:

- Makes external measurements or ingests only public information
- Doesn't control or have privileged access to agency systems
- A failure or compromise would not compromise the delivery of agency services

Examples:

- Basic upstream traffic filtering/DDoS (no decryption, negligible availability requirements)
- Basic CAPTCHA services on public facing non-sensitive sites and forms
- Public web analytics and uptime monitoring (Pingdom, StatusPage)
- Unauthenticated vulnerability and code scanning tools for public facing components or code

Out of Scope Detailed Example - Public Monitoring Tool: An agency uses an external service to monitor its non-critical public website/API availability via pings, logging uptime, and sending alerts.

> **Analysis:** Externally measures public endpoints; does not ingest or store sensitive federal data.

In Scope Detailed Example - Integrated Monitoring System: An agency integrates an Application Performance Monitoring (APM) service into its internal applications. This service collects sensitive federal data like distributed traces and detailed logs from internal sources, often via installed agents or privileged API access to other internal systems.

> **Analysis:** Handles internal, non-public federal information; possesses privileged access to internal systems.

Summary Table

Exclusion Category (from M-24-15, Sec 3)	**When FedRAMP Doesn't Apply (Core Condition)**	**Key Tests / Considerations**
1. Single Agency Systems: Info systems for only one agency's operations, hosted on cloud, not offered as a shared service or using a shared responsibility model	The service is exclusively for a single agency's operations and not intended for reuse or reconfiguration by other agencies	• Single agency has full operational & configuration responsibility • No assessment intended for reuse by others
2. Social Media & Communications Services: Used according to agency social media policies	The service is not an authoritative repository for federal information, and its unavailability would not result in the	• Used per agency policy (incl. Records Act) • Primary purpose: external communication • Not authoritative source for federal info

Exclusion Category (from M-24-15, Sec 3)	When FedRAMP Doesn't Apply (Core Condition)	Key Tests / Considerations
	loss of federal information	• All federal info within is intended for public use
3. Search Engines	The search engine is used primarily for public information discovery and does not store, index, or maintain internal federal information on behalf of the government	• Primary function: public info discovery • Does not collect/maintain federal info for agencies • Users instructed not to input sensitive federal info
4. Widely Available Commercial Information Services: Provide commercially available info to agencies; do not collect federal info (on behalf of the gov't)	The commercial information service does not collect or maintain federal information on behalf of the government	• Provides commercial services • May temporarily process fed info (e.g., address) but doesn't collect/maintain for the gov't • Agency never needs its info back from the service • Risk of exposure accepted (mission impact > exposure risk)
5. Ancillary Services (Negligible Risk): Compromise poses negligible risk to federal info/systems (e.g., external measurement, public info ingestion)	The agency determines through risk analysis that the failure or compromise of the ancillary service poses negligible risk to federal info and systems. Risk	• Makes external measurements or ingests only public info • Doesn't control or have privileged access to agency systems

Exclusion Category (from M-24-15, Sec 3)	When FedRAMP Doesn't Apply (Core Condition)	Key Tests / Considerations
	assessment is agency-specific	•A failure or compromise would not compromise the delivery of agency services